Trusted Process Classes

19th National Information Systems Security Conference

William L. Steffan

Tracor Applied Sciences, Incorporated

334-271-6804

Trusted Process Classes

Overview

- **BACKGROUND**
- **METHODOLOGY MOTIVATION**
- **DEFINITIONS**
- **TRUSTED PROCESS CLASS DISCRIMINATORS**
- **IMPLEMENTATION CONFINEMENT RULES**
- **SUMMARY**

Trusted Process Classes

BACKGROUND

- **VENDOR DILEMMA**
  - **Marketplace Pressures**
  - **NCSC Evaluation Hurdles**

- **DEVELOPER DILEMMA**
  - **Achieve Security Policy Compliance**
  - **Meet Operational Mission Requirements**

- **ASSURANCE DILEMMA**
  - **Trusted Process “Trustworthiness”**
  - **Common Framework for Understanding**

Methodology Motivation

- **ADDRESS DILEMMA PROBLEMS**
- **CODIFY “LESSONS LEARNED”**
- **PROMOTE COMMON UNDERSTANDING**
- **BRIDGE BETWEEN THEORY AND PRACTICE**
- **MAKE RULES EXPLICIT**

DEFINITIONS

- **TRUSTED PROCESS. A PROGRAM OR ALGORITHM WITH THESE CHARACTERISTICS:**
  - **May over-ride security policy enforcing mechanisms**
  - **Does not subvert security policy rules except in explicitly controlled, locally constrained ways**
  - **NEVER enforces globally applicable security policy rules**

Trusted Process Classes

Definitions (continue)

- **TRANQUILLITY PRINCIPLE. DIGITAL SECURITY LABEL REMAINS INVARIANT**

- **DISCRETIONARY ACCESS CONTROLS (DAC). "NEED-TO-KNOW" RULES**

- **MANDATORY ACCESS CONTROLS (MAC). "CLEARANCE" VERSUS "CLASSIFICATION" COMPROMISE PREVENTION RULES**

Trusted Process Classes

TRUSTED PROCESS CLASS DISCRIMINATORS

	OVERRIDE PRIVILEGE GRANTED			
TP Class	***Tranquillity***	***MAC***	***DAC***	***Action Permitted***
0	**---**	**---**	**---**	**Read Only**
1	**---**	**---**	**YES**	**R or W, R & W**
2	**---**	**YES**	**---**	**R or W, R & W**
3	**---**	**YES**	**YES**	**R or W, R & W**
4	**YES**	**---**	**---**	**R or W, R & W**
5	**YES**	**---**	**YES**	**R or W, R & W**
6	**YES**	**YES**	**---**	**R or W, R & W**
7	**YES**	**YES**	**YES**	**R or W, R & W**

Trusted Process Classes

IMPLEMENTATION CONFINEMENT RULES

PCR-1	Local Domain Context Storage
PCR-2	Local Domain Context Storage Purge
PCR-3	Trusted Process Audit
PCR-4	Assignment Statement Restrictions
PCR-5	Function or Subroutine Return Parameters
PCR-6	Least Privilege Principle Restrictions
PCR-7	Computational Expression Restrictions
PCR-8	Logical Expression Restrictions
PCR-9	Single Functionality Restrictions
PCR-10	Single Entry Restrictions
PCR-11	Single Entry Restrictions
PCR-12	Trusted Process Author
PCR-13	Configuration Management Restrictions
PCR-14	Trusted Process Qualification Testing

Trusted Process Classes

Summary

- **DEFINE TRUSTED PROCESS CLASSES**
- **TRUSTWORTHINESS MADE EXPLICIT**
- **CONFINEMENT RULES FOR IMPLEMENTORS**
- **ASSURANCES**
  - **Bridge between THEORY and PRACTICE**
  - **Meet SECURITY and MISSION REQUIREMENTS**
  - **Common understanding between SECURITY BIT-MEISTERS and SYSTEM DEVELOPERS**
- **BOTTOM LINE: *TRUST ... BUT VERIFY***